PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-041936
(43)Date of publication of application : 13.02.1998

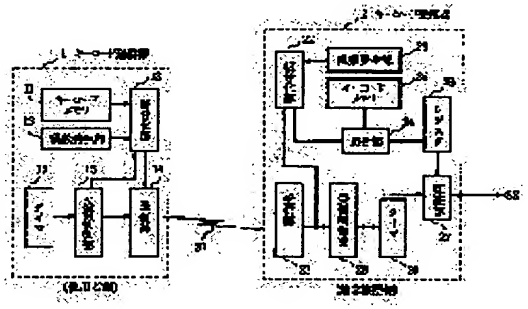
(51)Int.CI. H04L 9/32
G06F 1/00
H04Q 7/38
H04Q 9/00

(21)Application number : 08-190584
(22)Date of filing : 19.07.1996

(71)Applicant : NEC COMMUN SYST LTD
(72)Inventor : OSAI KAZUYA

(54) USER CERTIFICATION DEVICE FOR TERMINAL EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the operability, the security and the reliability by allowing a receiver to provide an output of a signal to set a terminal equipment to be in an available state when a key code registered in advance is collated with a received key code and the correctness of the key code is certified.
SOLUTION: A key code transmitter 1 is carried by the user of the terminal equipment. A ciphering section 13 ciphers a user key code registered in advance in a memory 11 by a random number. A transmission section 14 is controlled by a transmission control section 15 to send a ciphered key code signal S1 intermittently for a prescribed period. A key code receiver 2 is provided to the terminal equipment and sends a signal S2 to set the terminal equipment to be in an unavailable state as a default at application of power. A reception section 21 is controlled by a reception control section 28 and receives the key code signal S1 with intermittent reception. A collation section 25 collates a key code registered in a key code memory 25 with a key code decoded by a decoding section 22. A certification section 27 sends an output signal S2 to set the terminal equipment to be in an available state when certifying the key code through a plurality of collation results stored in a register 26.



LEGAL STATUS

[Date of request for examination] 19.07.1996
[Date of sending the examiner's decision of rejection] 01.02.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－41936

(43)公開日　平成10年(1998)２月13日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７３Ｅ
Ｇ０６Ｆ	1/00	３７０		Ｇ０６Ｆ	1/00	３７０Ｅ
Ｈ０４Ｑ	7/38			Ｈ０４Ｑ	9/00	３０１Ｚ
	9/00	３０１				３０１Ｂ
				Ｈ０４Ｂ	7/26	１０９Ｒ

審査請求　有　請求項の数６　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平8－190584

(22)出願日　平成８年(1996)７月19日

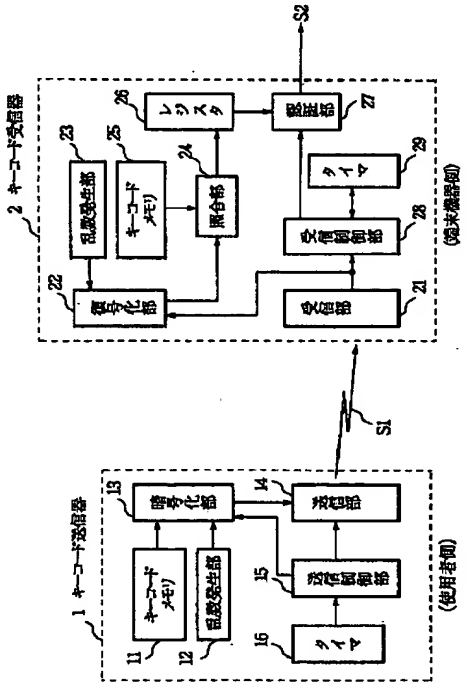
(71)出願人　000232254
日本電気通信システム株式会社
東京都港区三田１丁目４番28号

(72)発明者　小佐井　一哉
東京都港区三田一丁目４番28号　日本電気通信システム株式会社内

(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　端末機器の使用者認証装置

(57)【要約】
【課題】操作性およびセキュリティ、信頼性を向上する。
【解決手段】キーコード送信器１は端末機器の使用者により携帯される。暗号化部１３は、メモリ１１に予め登録済の使用者キーコードを、乱数により暗号化する。送信部１４は、送信制御部１５によって制御され、暗号化されたキーコード信号Ｓ１を一定周期で間欠的に送信する。キーコード受信器２は端末機器に設けられ、電源オン時の初期値として端末機器を使用不可状態に設定する信号Ｓ２を送出する。受信部２１は受信制御部２８によって制御され、間欠的に受信動作を行ってキーコード信号Ｓ１を受信する。照合部２５は、キーコードメモリ２５に登録済のキーコードと復号化部２２により復号されたキーコードとを照合する。認証部２７は、レジスタ２６に保持された複数の照合結果によりキーコードを認証できたときに、端末機器を使用可状態に設定する出力信号Ｓ２を送出する。



1

【特許請求の範囲】

【請求項１】　使用者が携帯し予め付与されたキーコードを送信する送信器と、この送信器が送信する前記キーコードを受信し認証する受信器とを備え、前記受信器は、予め登録済のキーコードと受信した前記キーコードとを照合して正しいものと認証できたときに端末機器を使用可能状態に設定する信号を出力する認証手段を有していることを特徴とする端末機器の使用者認証装置。

【請求項２】　前記送信器は一定周期で間欠的に前記キーコードを送信する手段を有し、前記受信器は前記送信器の送信周期に同期して前記キーコードを受信する手段を有していることを特徴とする請求項１記載の端末機器の使用者認証装置。

【請求項３】　前記送信器は前記キーコードを乱数により暗号化する手段を有し、前記受信器は前記暗号化手段により前記暗号化されたキーコードを復号化する手段を有していることを特徴とする請求項２記載の端末機器の使用者認証装置。

【請求項４】　前記暗号化手段は前記キーコードを送信する毎に異なる乱数テーブルを使用して暗号化し、前記復号化手段は前記暗号化手段が使用したのと同じ乱数テーブルにより復号化することを特徴とする請求項３記載の端末機器の使用者認証装置。

【請求項５】　前記暗号化手段は使用した乱数テーブルを示す情報を前記暗号化されたキーコードと共に送出し、前記復号化手段は前記乱数テーブルを示す情報に基づき前記暗号化されたキーコードを復号化することを特徴とする請求項４記載の端末機器の使用者認証装置。

【請求項６】　前記受信器の前記認証手段は、受信した複数のキーコードの照合結果が所定回数連続して一致したときに正しいものと認証することを特徴とする請求項２記載の端末機器の使用者認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は端末機器の使用者認証装置に関し、特に携帯電話機や携帯型パソコン等の端末機器が他人によって不正に使用されるのを防止する使用者認証装置に関する。

【０００２】

【従来の技術】従来のこの種の技術は、例えば、特開平４－２３３８９２号公報に示されているように、リモコン操作器から機器に対して所定の指令を送信し、この指令を機器に受信確認させることにより、機器を動作禁止状態にしている。

【０００３】

【発明が解決しようとする課題】しかし、上述した従来技術では、機器を動作禁止状態に設定するためには、リモコン操作器を操作しなければならず、また、リモコン操作器によって機器の動作禁止状態が解除されないように、リモコン操作器を隠したり、別の場所に運んだりしなければならない。従って、操作が煩わしいばかりでなく、リモコン操作を忘れたり、リモコン操作器を放置したままにする可能性があり、操作性、信頼性に欠けるという問題点を有している。

2

【０００４】本発明の目的は、端末機器が不正に使用されるのを防止する使用者認証装置の、操作性、セキュリティおよび信頼性を向上することにある。

【０００５】

【課題を解決するための手段】本発明の端末機器の使用者認証装置は、使用者が携帯するキーコード送信器から周期的に暗号化されたキーコードを送信し、端末機器側に設けたキーコード受信器によって受信し、正しいと認証できたときに端末機器を使用可能状態にする信号を出力する。またキーコードを送信する毎に異なる乱数テーブルを使用して暗号化し、更に、受信した複数のキーコードの照合結果により認証することにより、セキュリティおよび信頼性を向上する。

【０００６】具体的には、使用者が携帯し予め付与されたキーコードを送信する送信器と、この送信器が送信する前記キーコードを受信し認証する受信器とを備え、前記受信器は、予め登録済のキーコードと受信した前記キーコードとを照合して正しいものと認証できたときに端末機器を使用可能状態に設定する信号を出力する認証手段を有している。また、前記送信器は一定周期で間欠的に前記キーコードを送信する手段を有し、前記受信器は前記送信器の送信周期に同期して前記キーコードを受信する手段を有している。前記送信器は前記キーコードを乱数により暗号化する手段を有し、前記受信器は前記暗号化手段により前記暗号化されたキーコードを復号化する手段を有している。

【０００７】更に、前記暗号化手段は前記キーコードを送信する毎に異なる乱数テーブルを使用して暗号化してよく、この場合、使用した乱数テーブルを示す情報を前記暗号化されたキーコードと共に送出し、前記復号化手段は前記乱数テーブルを示す情報に基づき前記暗号化されたキーコードを復号化してもよい。また、前記受信器の前記認証手段は、受信した複数のキーコードの照合結果が所定回数連続して一致したときに正しいキーコードであると認証するようにしてもよい。

【０００８】

【発明の実施の形態】次に本発明について図面を参照して説明する。

【０００９】図１は本発明の一実施形態を示す構成図である。キーコード送信器１は、予め設定された使用者のキーコードを送信する携帯可能な小型化されたキーコード送信器であり、端末機器を使用する際に使用者によって常に携帯される。

【００１０】キーコード受信器２は、端末機器側に設けられており、キーコード送信器１から送信される使用者のキーコード信号Ｓ１を受信し、受信したキーコードが

正しいものと認証できたときに端末機器を使用可状態に設定する出力信号Ｓ２を送出する。また、受信したキーコードが認証できなかったときには端末機器を使用不可状態に設定する出力信号Ｓ２を送出する。端末機器は、キーコード受信器２の出力信号Ｓ２に応じて使用可状態または使用不可状態になる。

【００１１】キーコード送信器１は、消費電力の節減をはかるために一定周期で間欠的にキーコード信号Ｓ１を送信するように構成されており、使用者のキーコードを予め記憶しているキーコードメモリ１１と、キーコードを暗号化するための乱数を生成する乱数発生部１２と、キーコードを乱数により暗号化して図３に示すようなキーコード信号を生成する暗号化部１３と、キーコード信号を電波として送信する送信部１４と、消費電力の節減をはかるためにタイマ１６に応じて間欠的にキーコード信号を送信するように送信部１４を制御すると共に、所定のキーコード信号を生成するように暗号化部１３を制御する送信制御部１５とを有している。

【００１２】キーコードメモリ１１としては書き込み可能なＲＯＭ（例えばフラッシュ・ロム等）を使用し、キーコード送信器１またはキーコード受信器２が紛失した場合に、新しいキーコードが書き込めるようにしておく。暗号化の手段としては、例えば、キーコードと乱数のビット数を同じにしておき、キーコードと乱数との排他的論理和をとれるようにしてもよい。

【００１３】一方、キーコード受信器２は、キーコード送信器１から送信されたキーコード信号Ｓ１を受信する受信部２１と、送信側で使用された乱数と同じ乱数を乱数発生部２３から受け暗号化されたキーコードを復号する復号化部２２と、キーコードメモリ２５に予め登録されているキーコードおよび復号されたキーコードを照合する照合部２４と、照合部２４の照合結果を過去の分も含めて保持するレジスタ２６と、レジスタ２６に保持されている照合結果に基づき使用者の正しいキーコードであるか否かを認証し、正しいものと認証できたときに端末機器の使用可を指示する出力信号Ｓ２を送出する認証部２７と、消費電力の節減をはかるためにタイマ２９に応じて間欠的にキーコード信号を受信するように受信部２１を制御すると共に、キーコードを復号する復号化部２２を制御する受信制御部２８とを有している。

【００１４】なお、送信制御部１５および受信制御部２１には、マイコンやＤＳＰ（ディジタル・シグナル・プロセッサ）等を使用して各種制御処理を実行させてもよい。

【００１５】図３は、キーコード送信器１から送信されるキーコード信号のフォーマット例を示している。同図（ａ）は第１のフォーマット例であり、送受信の同期用の同期フレーム、暗号化の乱数を指定する乱数テーブル番号、暗号化されたキーコード、エラー訂正用のパリティビットにより構成されている。また、同図（ｂ）は第２のフォーマット例であり、信号の先頭を示すスタートビット、暗号化されたキーコード、エラー訂正用のパリティビット、信号の末尾を示すストップビットにより構成されている。

【００１６】ところで、キーコード送信器１から一定周期で間欠的に送信されるキーコード信号を、キーコード受信器２が受信するためには、送信側のタイマ１６と受信側のタイマ２９とを同期させる必要がある。このため、キーコード信号には、同期フレーム（図３（ａ）の場合）あるいはスタートビット、ストップビットを（図３（ｂ）の場合）を配置している。受信制御部２１は、キーコード信号の同期フレームあるいはスタートビット、ストップビットを検出してタイマ２９を制御する。なお、同期フレームは特定のビットパターンである。また、スタートビットは、例えば、レベル「１」の一定数のビット列とすれば、ストップビットは、例えば、レベル「０」の一定数のビット列である。

【００１７】また、キーコード送信器１が乱数により暗号化したキーワードを、キーコード受信器２で復号化するためには、送信側で使用された乱数と同じ乱数を受信側で使用する必要がある。例えば、キーコード信号の送信毎に異なる乱数を使用する場合は、乱数発生部１２，２３に複数の異なる乱数テーブルをそれぞれ記憶させておき、キーコード信号の送信毎に乱数テーブルを選択させ、選択した乱数テーブルの番号を、図３（ａ）に示したように、キーコード信号に含めて送信し、受信制御部２１が乱数テーブル番号を検出して復号化部２２に通知すればよい。なお、常に同じ乱数を繰り返し使用する場合は、乱数発生部１２，２３に同じ一つの乱数テーブルをそれぞれ記憶させておけばよく、例えば図３（ｂ）に示したように、乱数に関する情報をキーコード信号に含めなくてもよい。復号化の手段としては、例えば、送信側においてキーコードと乱数との排他的論理和をとって暗号化したのであれば、受信側では、暗号化に使用されたのと同じ乱数と暗号化されたキーコードとの排他的論理和をとればよい。

【００１８】次に動作を説明する。

【００１９】図２（ａ）はキーコード送信器１の動作を示すフローチャートである。端末機器の使用者が携帯するキーコード送信器の電源をオンすることにより動作を開始する（ステップ１０１）。使用者のキーコードをキーコードメモリ１１から読み出して暗号化部１３へ送出し保持させる（ステップ１０２）。また、乱数発生部１２が生成する乱数を暗号化部１３へ送出し（ステップ１０３）、乱数によりキーコードを暗号化する（ステップ１０４）。暗号化されたキーコードを含むキーコード信号をタイマに応じて一定周期で間欠的に送信する（ステップ１０５，１０６）。キーコード信号を送信する毎にステップ１０３からステップ１０６の処理を繰り返す。

【００２０】図２（ｂ）はキーコード受信器２の動作を

示すフローチャートである。最初に、キーコード受信器の電源がオンされたとき（ステップ２０１）、初期値として端末機器を使用不可状態に設定する信号を送出する（ステップ２０２）。その後、消費電力節減のために一定周期で間欠的に受信動作を行い、暗号化されたキーコードを受信すると（ステップ２０３）、復号化部２２は該当する乱数を読み出し（ステップ２０４）、キーコードを復号する（ステップ２０５）。照合部２５は、登録してあるキーコードをキーコードメモリ２５から読み出し（ステップ２０６）、復号化したキーコードと照合し（ステップ２０７）、一致したか否かの照合結果を過去のものを含めてM（Mは３以上の整数）個以上をレジスタ２６に保持する（ステップ２０８）。

【００２１】キーコードの受信周期毎に（ステップ２０９）、レジスタ２６に保持された照合結果をチェックし（ステップ２１０）、一致を示す照合結果がM（Mは３以上の整数、例えばM＝５）回連続したならば、端末機器を使用可状態に設定する信号を送出した後（ステップ２１１）、ステップ２０４からの処理を繰返す。また、一致を示す照合結果が２～（M－１）回連続したならば、ステップ２０４からの処理を繰返す。一致を示す照合結果が連続しないならば（ステップ２１２）、端末機器を使用不可状態に設定する信号を送出する（ステップ２１３）。

【００２２】このようにすることにより、一旦、端末機器が使用可状態に設定されたならば、その後、一致を示す照合結果が所定回数連続しなければ端末装置を使用可状態にしないので、信号伝送上の間欠障害が発生しても、直ちに端末機器が使用不可状態に切替わることはない。万一、同一周波数の妨害信号を受信し、且つキーコードが一致したとしても、このような信号を連続して受信する可能性は低いので、セキュリティおよび信頼性を向上できる。

【００２３】なお、上述した実施形態では、キーコード送信器１およびキーコード受信器２の両方にタイマを設けて送受信の同期をとっているが、いずれか一方にタイマを設け、同期情報を他方に通報して同期するようにしてもよい。

【００２４】

【発明の効果】以上説明したように本発明によれば、使用者が携帯するキーコード送信器から周期的に暗号化されたキーコードを送信し、端末機器側に設けたキーコード受信器によって受信し、正しいと認証できたときに端末機器を使用可能状態にする信号を出力することにより、端末機器と使用者とが一定距離以上離れ場合や、キーコード送信器の電源を切った場合には、端末機器を自動的に使用不可状態にするにことができるので、従来例のような操作を必要とせず、操作性および信頼性を向上できる。

【００２５】また、キーコードを送信する毎に異なる乱数テーブルを使用して暗号化し、更に、受信した複数のキーコードが所定回数連続して一致したときに認証することにより、セキュリティおよび信頼性を更に向上できる。

【図面の簡単な説明】

【図１】本発明の一実施形態を示す構成図である。

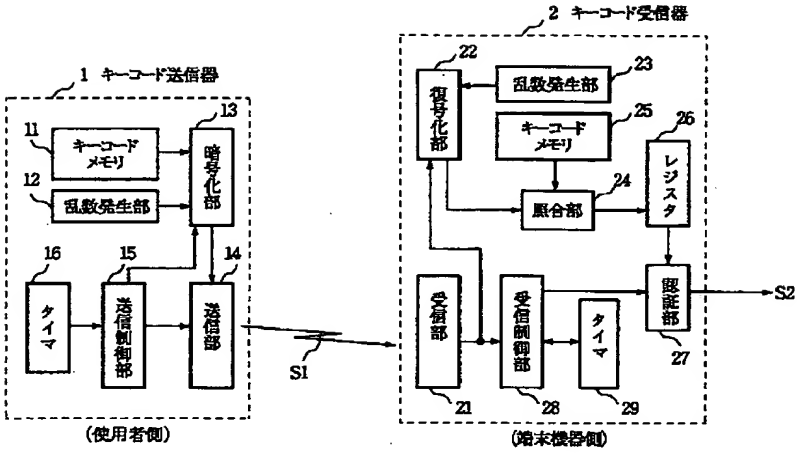
【図２】図１に示したキーコード送信器１およびキーコード受信器２の動作を示すフローチャートである。

【図３】図１に示したキーコード送信器１から送信されるキーコード信号のフォーマット例を示す図である。

【符号の説明】

１　キーコード送信器
２　キーコード受信器
１１，２５　キーコードメモリ
１２，２３　乱数発生部
１３　暗号化部
１４　送信部
１５　送信制御部
１６，２９　タイマ
２１　受信部
２２　復号化部
２４　照合部
２６　レジスタ
２７　認証部
２８　受信制御部
１０１～１０６　キーコード送信器１の動作を示すステップ
２０１～２１３　キーコード受信器２の動作を示すステップ

【図１】



【図３】

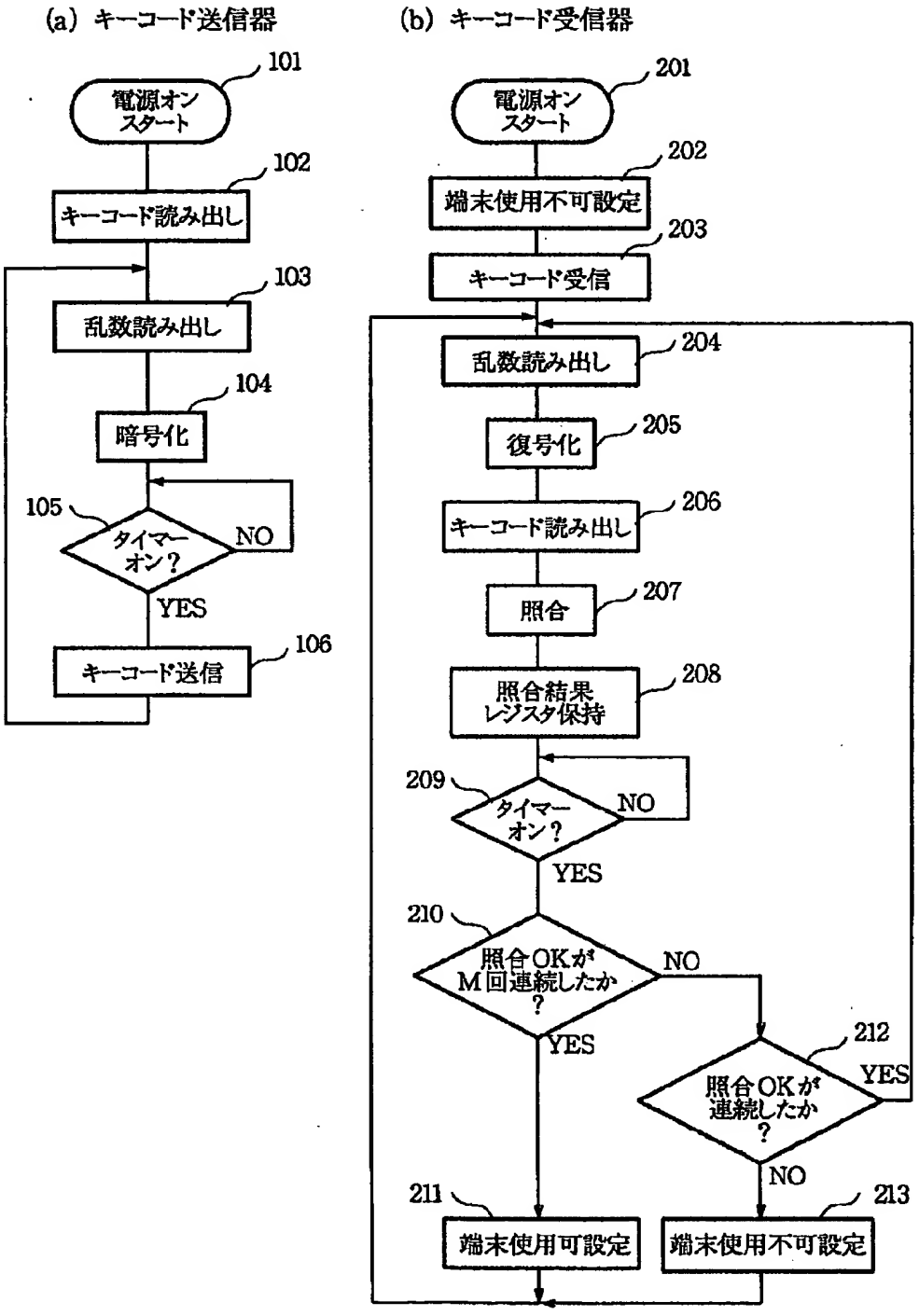
(a)

同期フレーム	乱数テーブル番号	キーコード	パリティ

(b)

スタートビット	キーコード	パリティ	ストップビット

【図２】


(a) キーコード送信器
101
電源オン スタート
102
キーコード読み出し
103
乱数読み出し
104
暗号化
105
タイマーオン？
NO
YES
106
キーコード送信
(b) キーコード受信器
201
電源オン スタート
202
端末使用不可設定
203
キーコード受信
204
乱数読み出し
205
復号化
206
キーコード読み出し
207
照合
208
照合結果レジスタ保持
209
タイマーオン？
NO
YES
210
照合OKがM回連続したか？
NO
YES
212
照合OKが連続したか？
YES
NO
211
端末使用可設定
213
端末使用不可設定

フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
			Ｈ０４Ｌ	9/00	６７３Ｂ
					６７３Ｃ